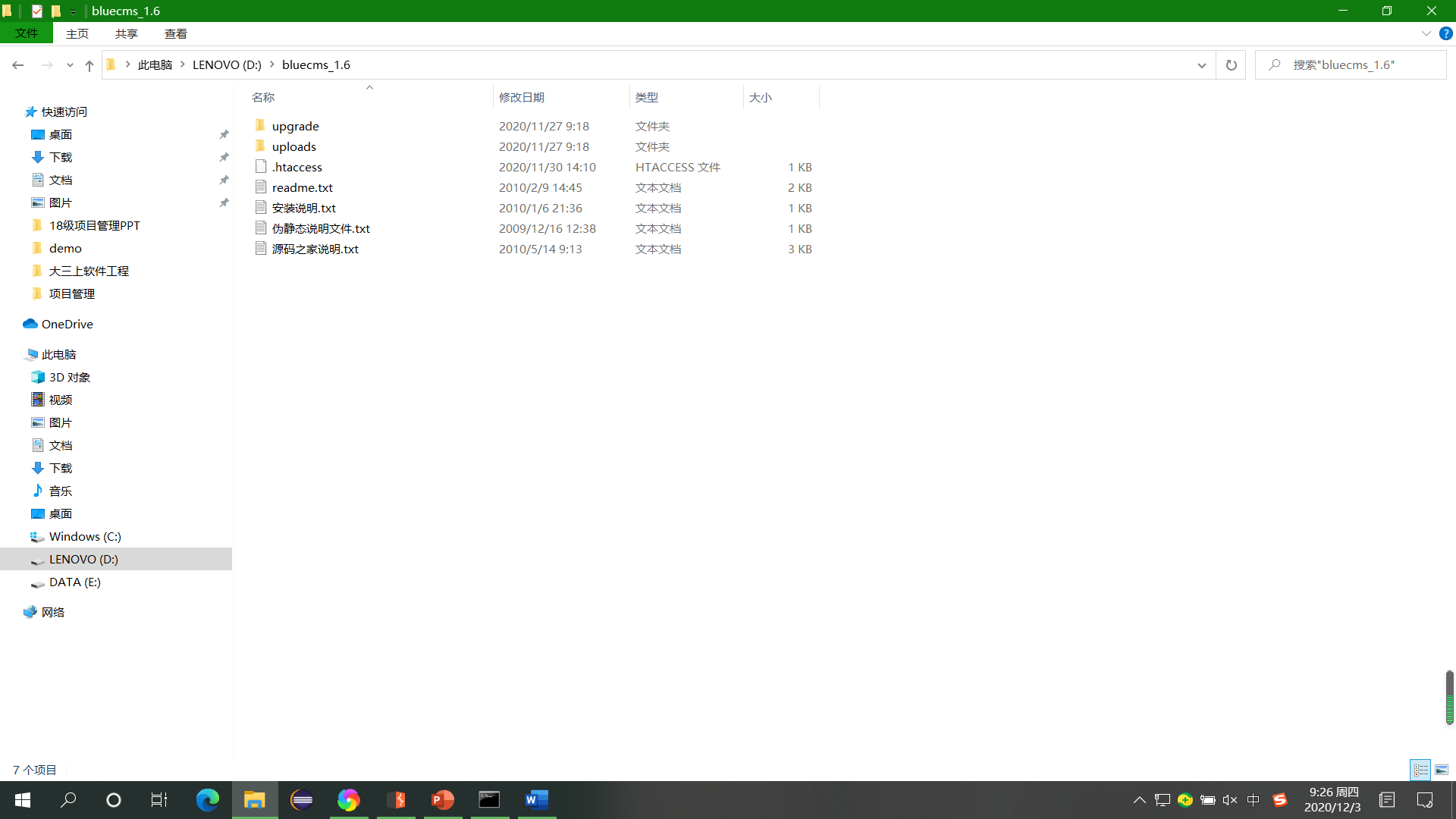
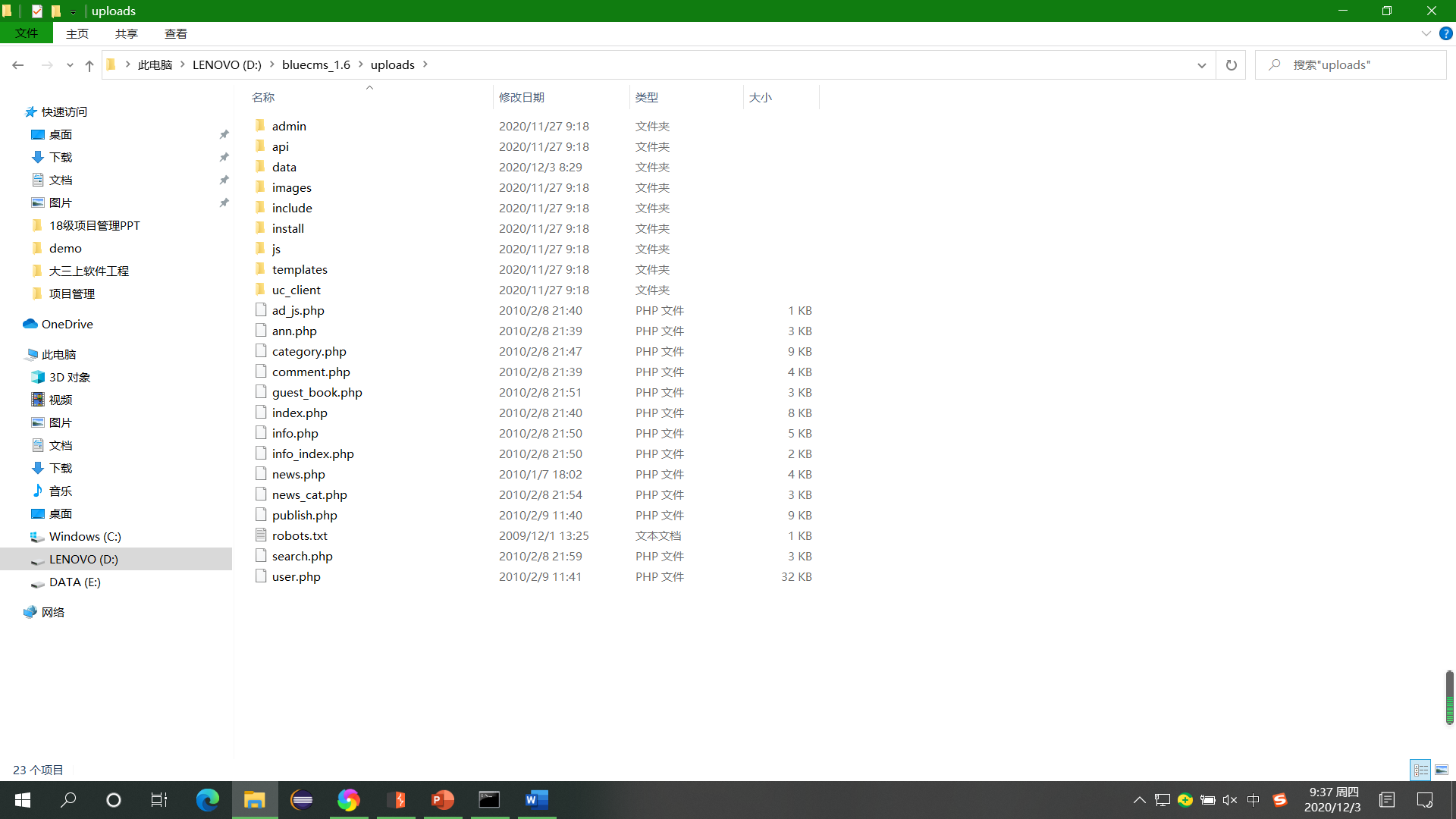
**渗透测试**

1. 信息收集
2. 域名信息

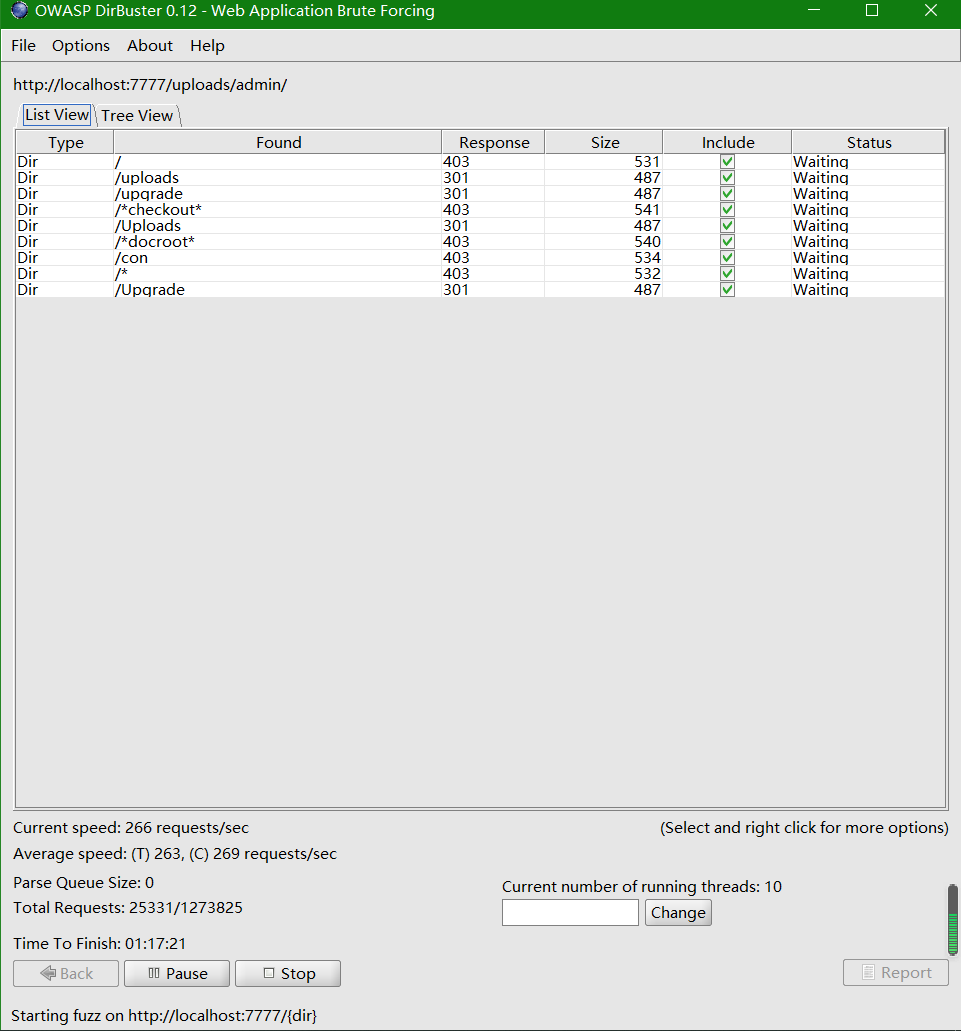
IP地址 10.7.86.241

1. 敏感目录

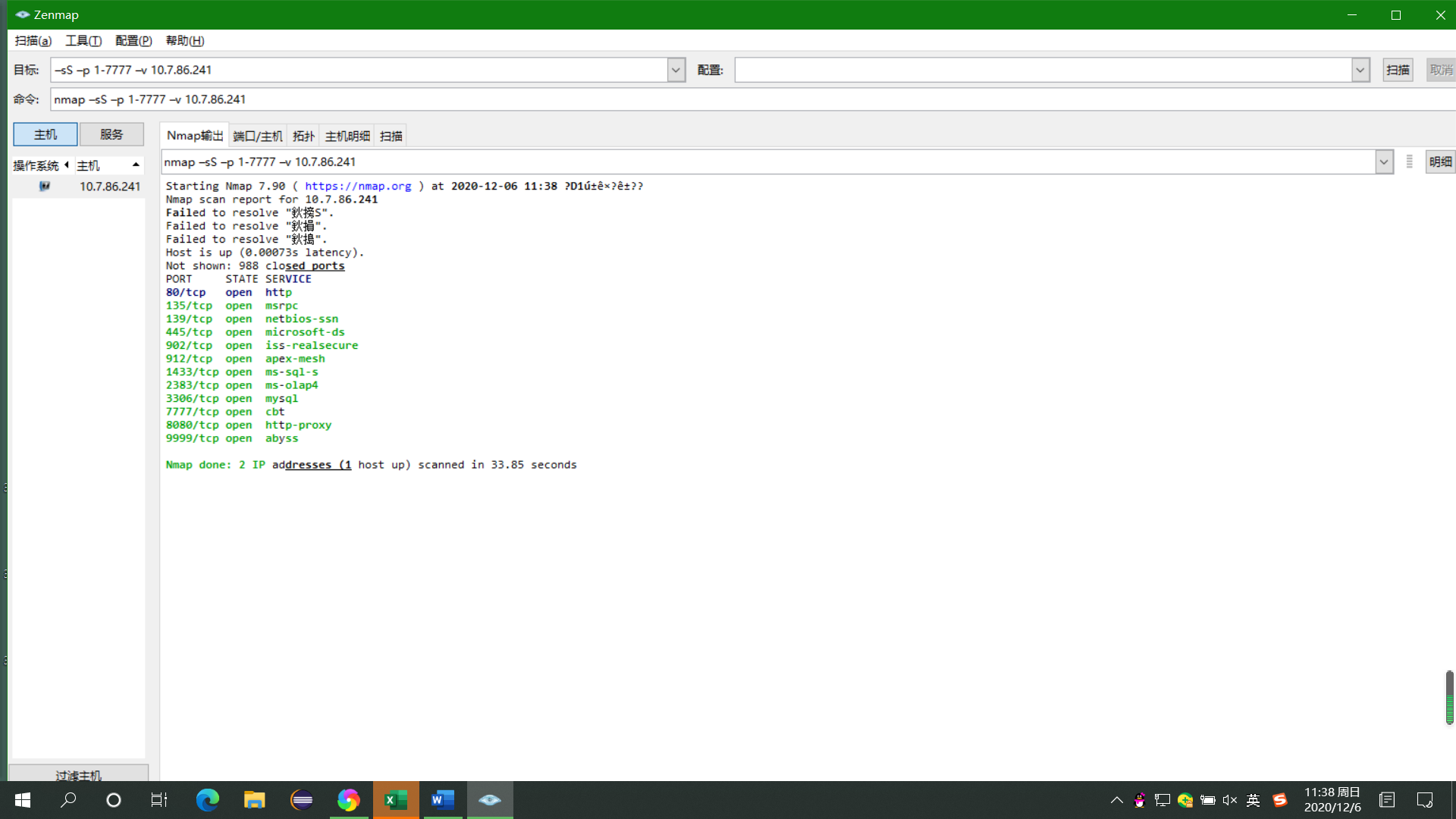


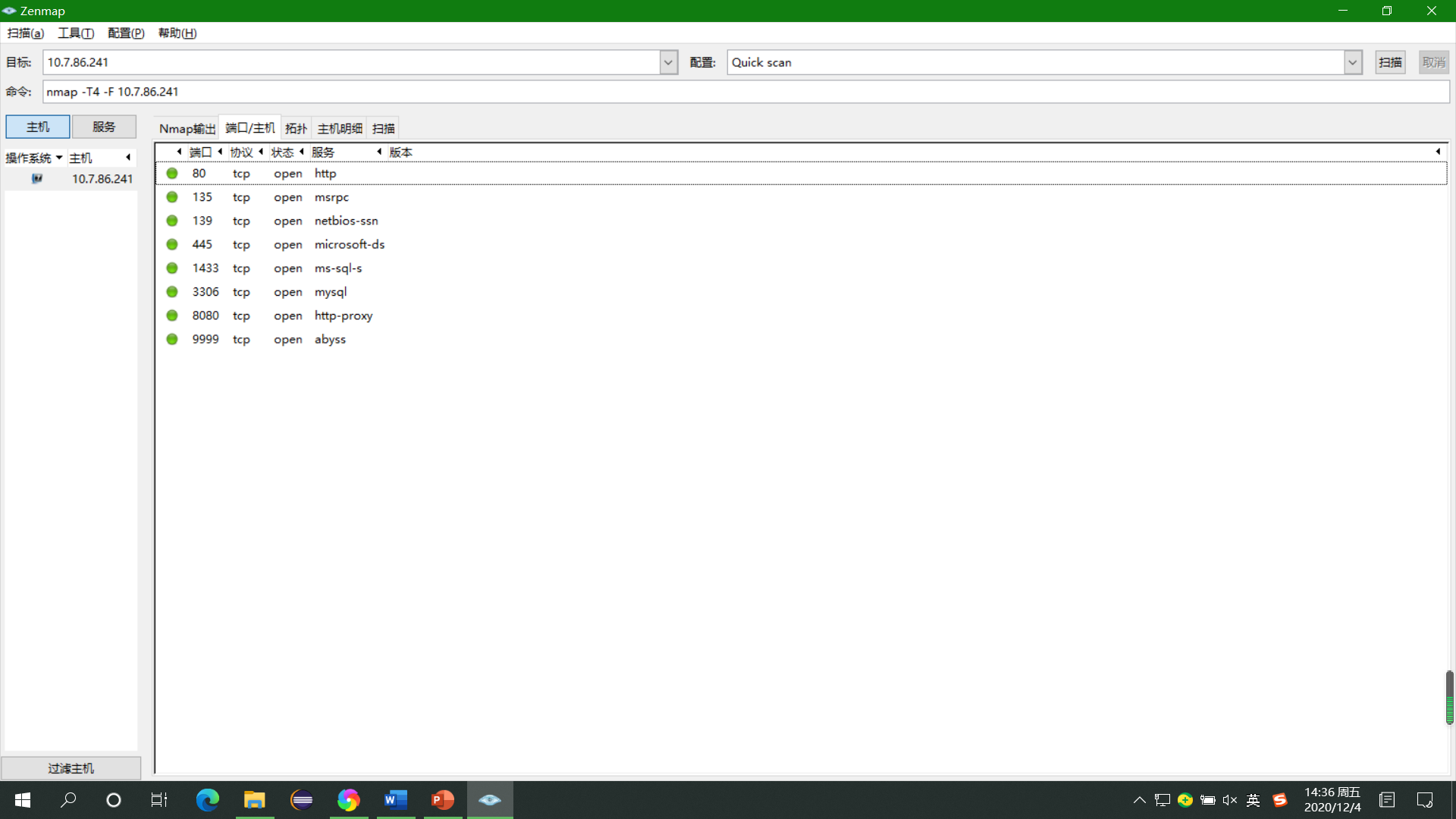


借助DirBuster工具进行敏感目录和隐藏文件的扫描：



借助Zenmap进行端口扫描：





1. 整站分析

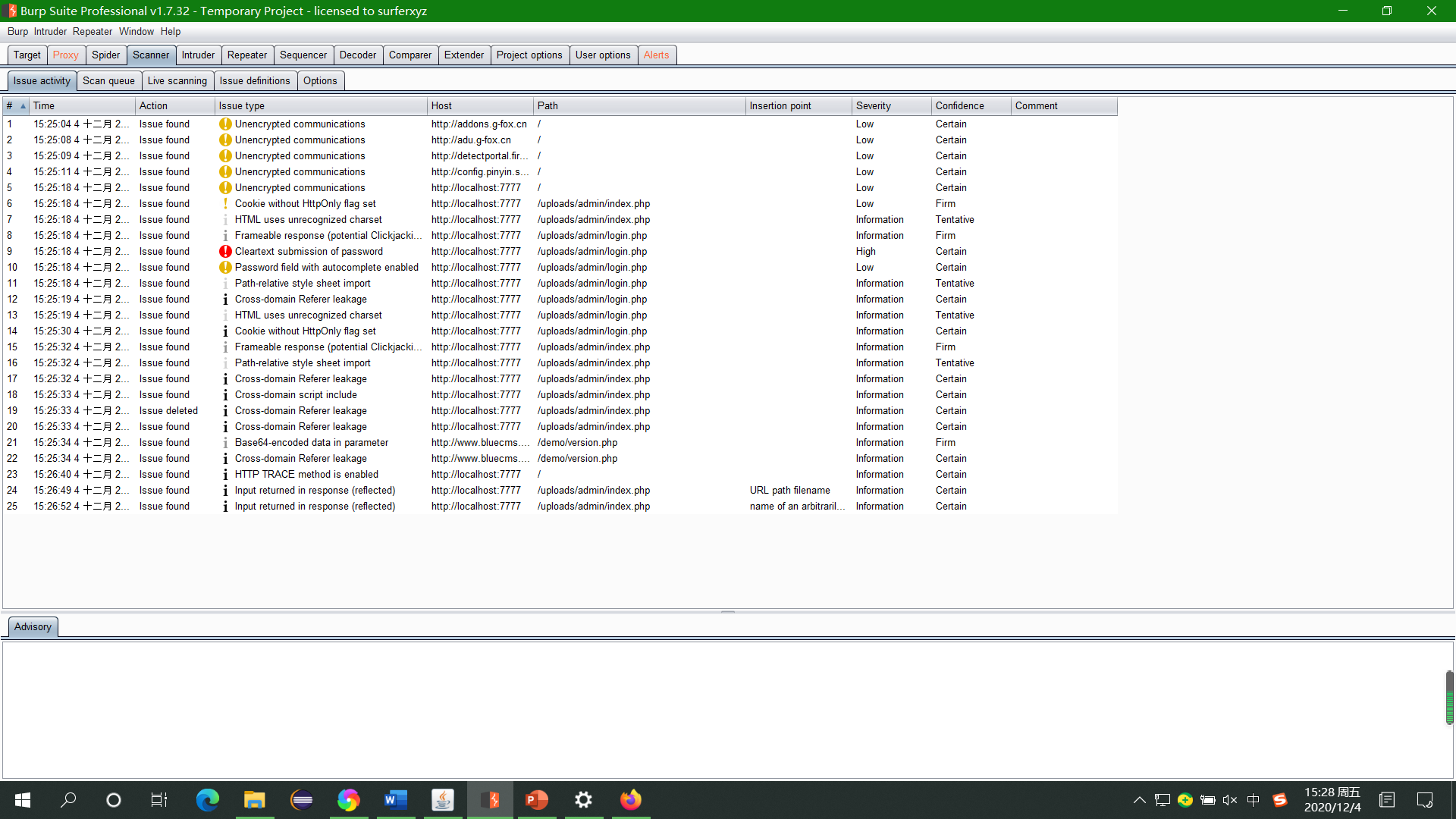
使用Windows系统，因为URL中字母大写仍能访问

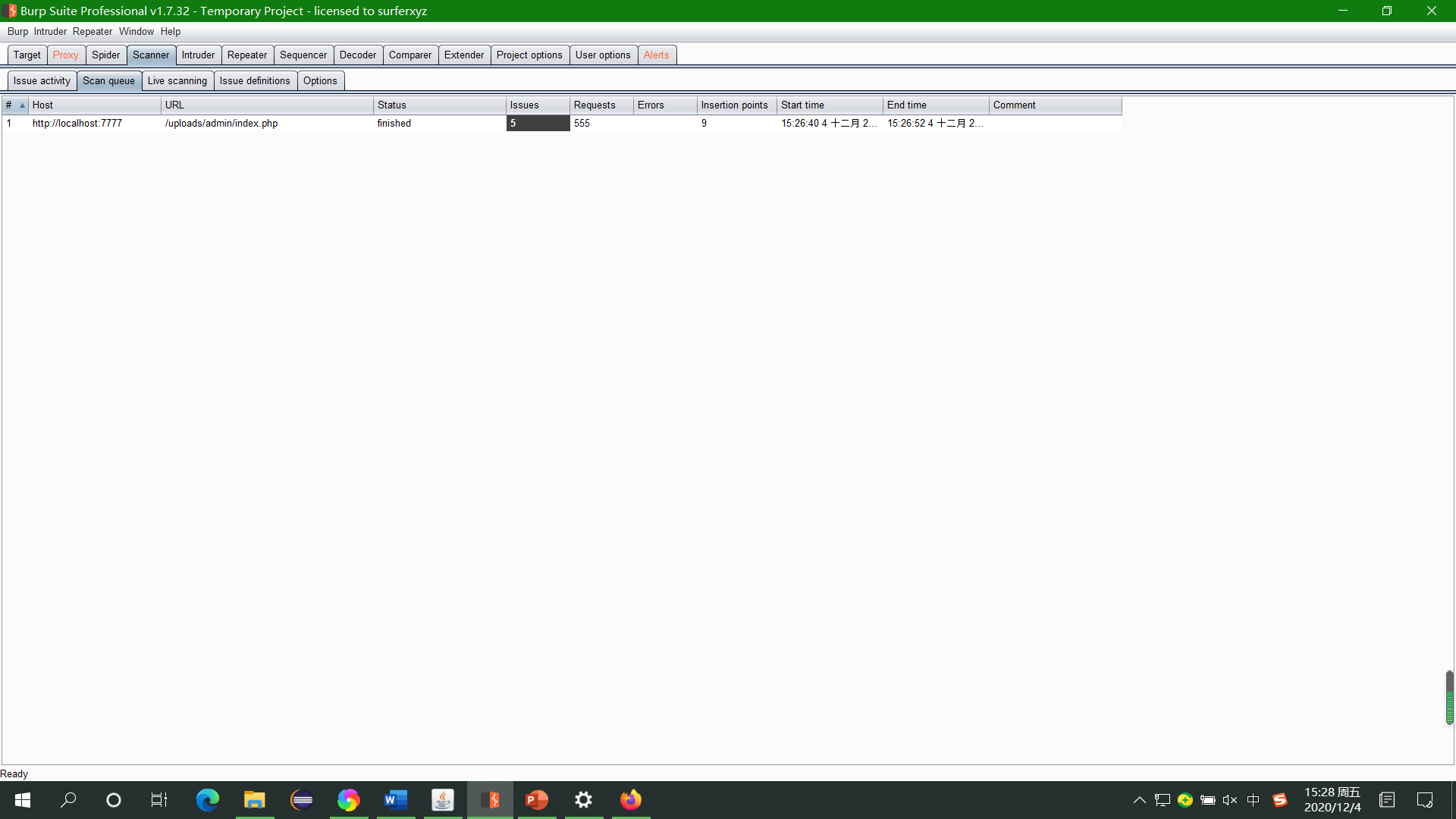
脚本类型PHP脚本，因为URL后有.php

服务器软件：Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

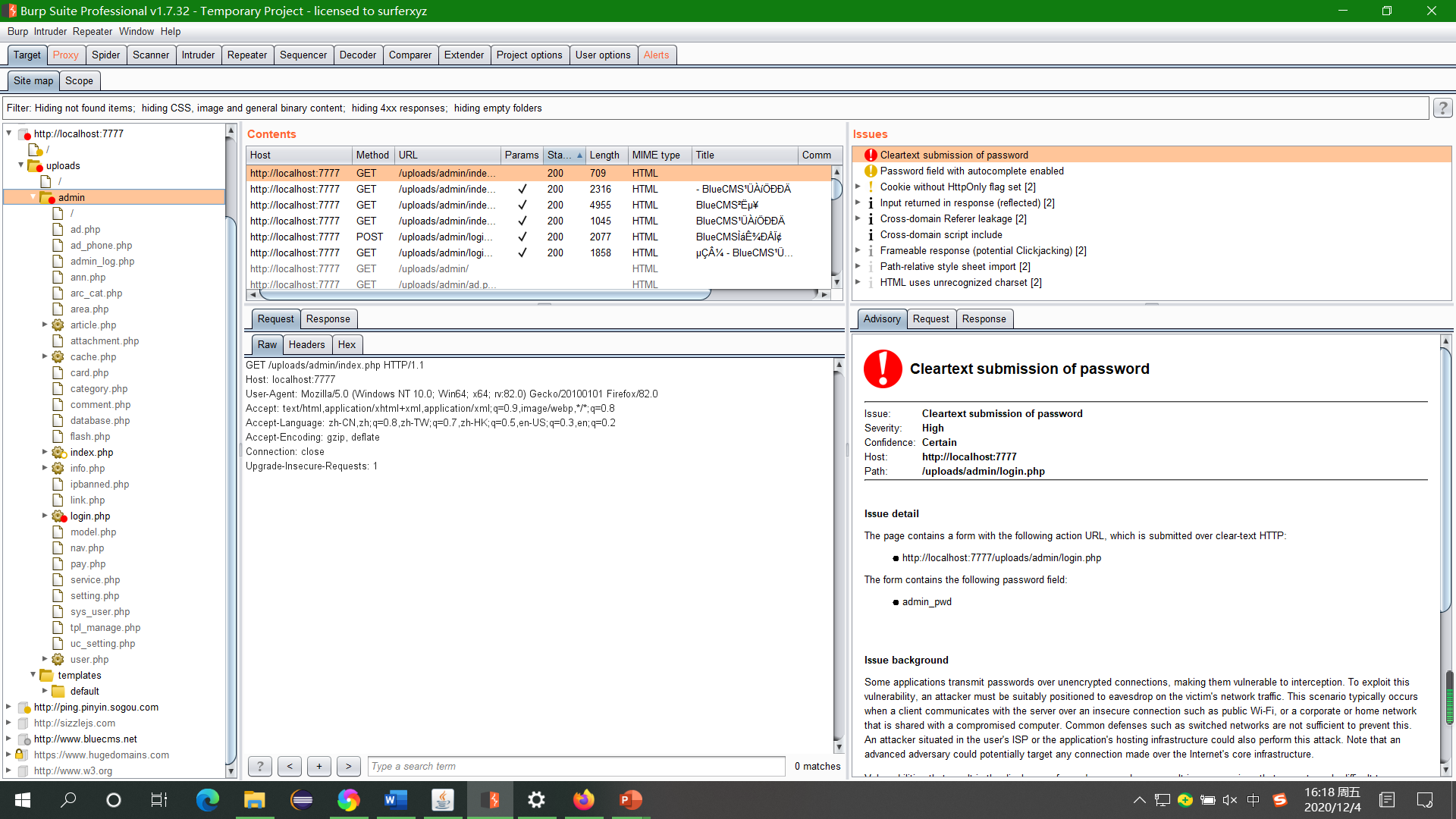
使用MySQL 版本5.7.26

1. 使用BurpSuite漏洞扫描



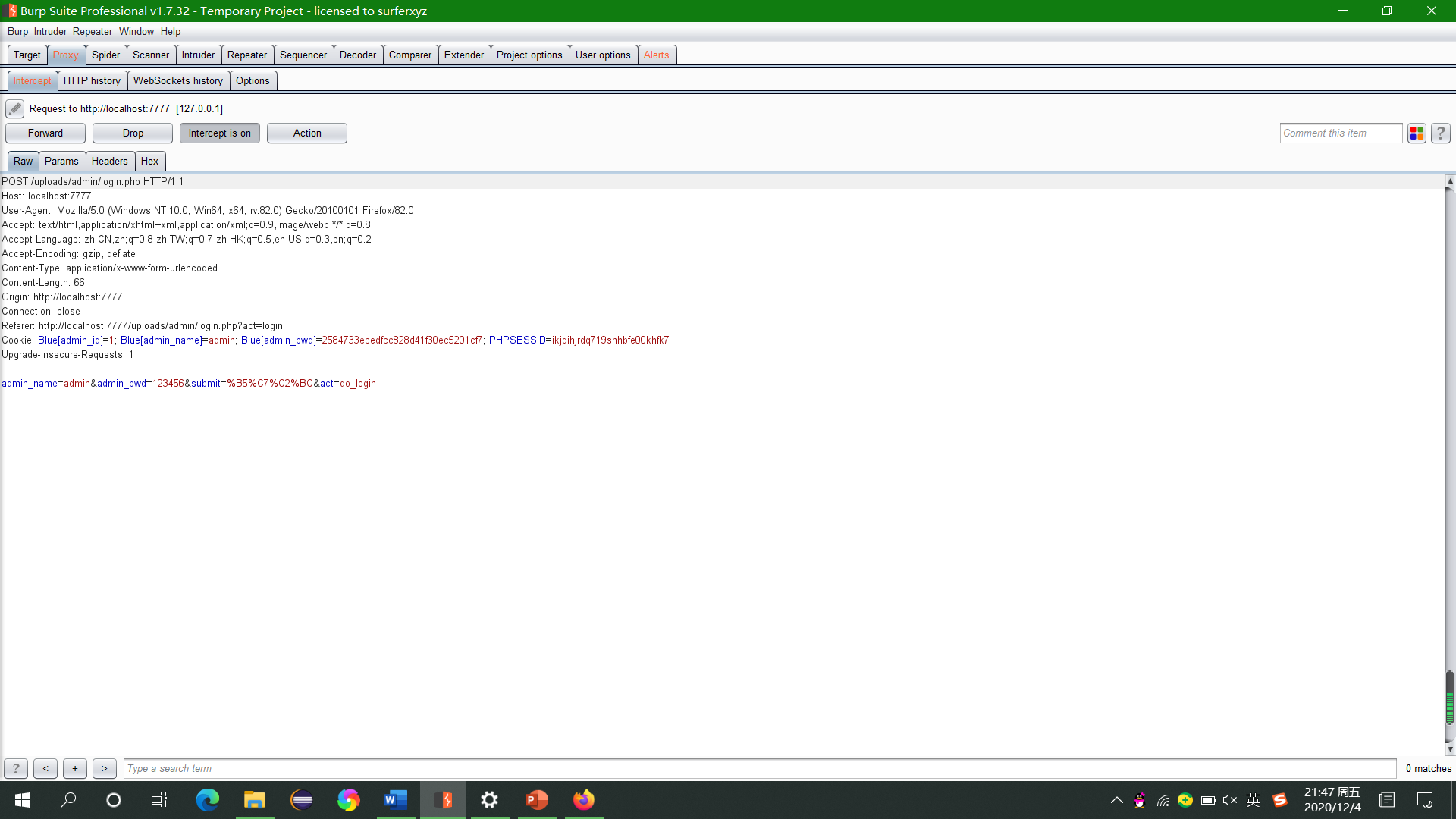


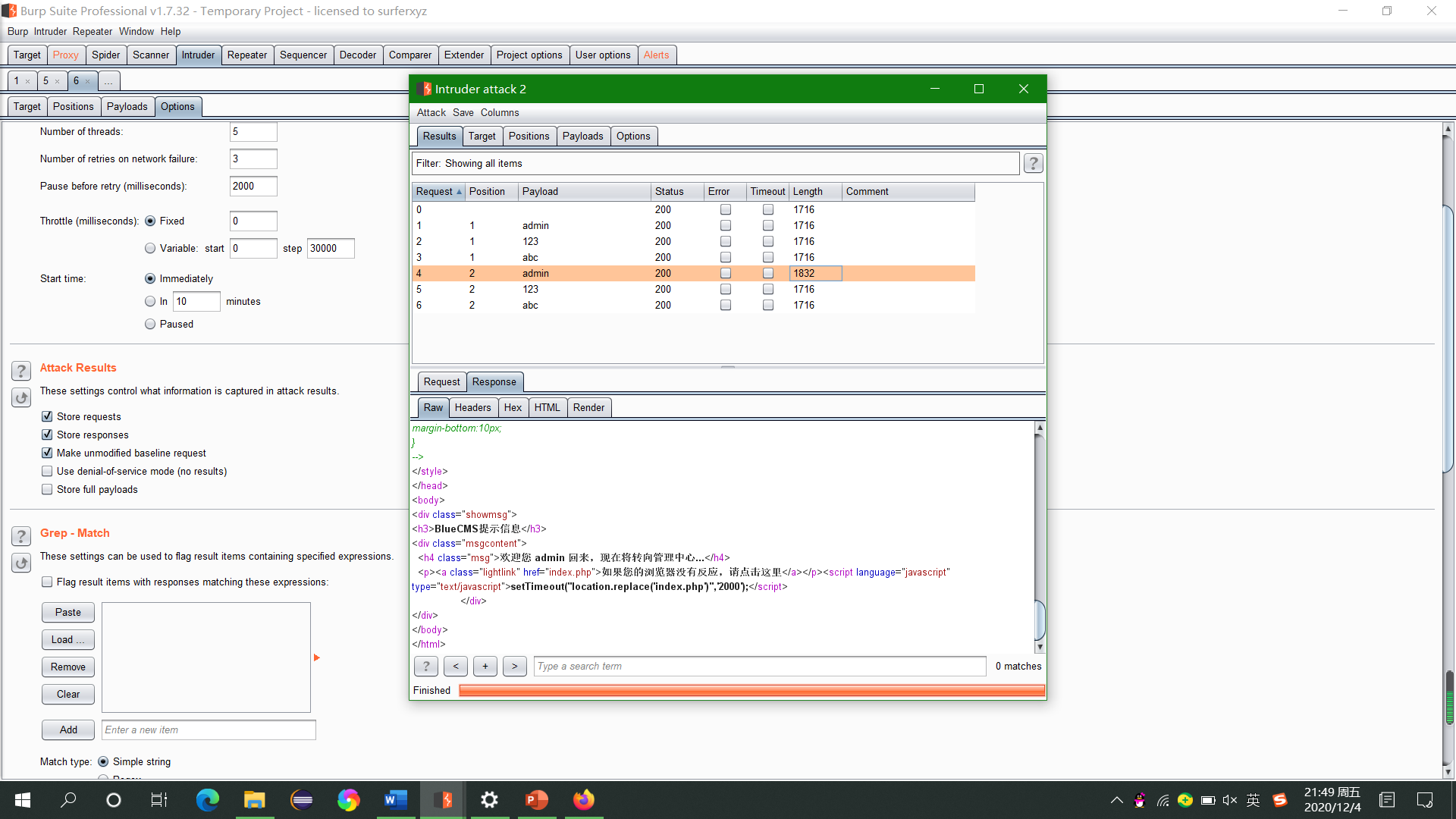
1. 爬取网站



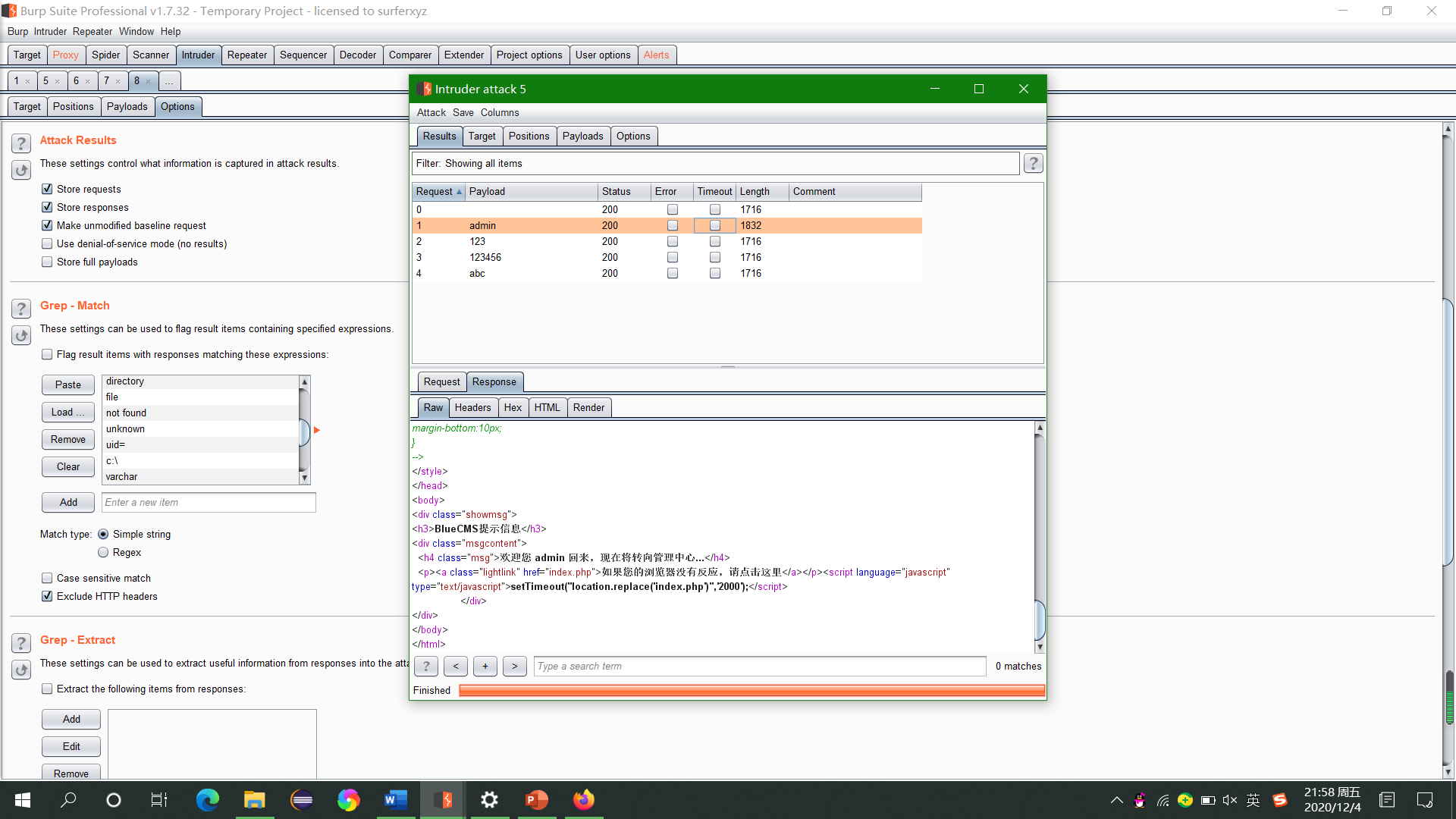
抓包：

（1）Sniper





(2)Battering ram:



4、手工渗透测试

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **模块** | **用例名** | **前提** | **步骤** | **预期结果** | **实际结果** |
| 后台-登录 | 使用弱密码库爆破管理员账号密码 | 打开后台 | 进入后台登录页面，输入随机的用户名和密码 | 无法登录成功 | 能够使用admin/admin登陆成功 |
| ad\_js.php | SQL注入漏洞 | 打开前台 | 在地址栏输入<http://localhost:7777/ad_js.php?ad_id=1> UNION SELECT 1,2,3,4,5,6,GROUP\_CONCAT(admin\_name,0x3a,pwd)FROM blue\_admin | 无法发现用户名和密码 | 在源代码中能查看到用户名和密码 |
| 前台-登录 | 网站根目录下文件读取 | 打开前台 | 前端网站用户在正常登陆的时候，输入值变量可以控制，可以嵌入base64加密代码，将用户登录代码函数的变量更改，进行抓包  用户登陆代码里的某个函数发现变量可以任意的更改，我们抓包测试 | 无法访问网站根目录下的文件 | 能够访问到网站根目录下的任意文件 |
| 前台-个人资料-邮箱 | 反射型XSS | 打开前台 | 登录后，点击个人资料，修改邮箱地址中输入<script>alert(安全测试)</script> | 提示错误信息 | 管理员打开后台会出现弹窗 |